NORTEL

Solution Brief

Nortel WLAN 2300 Series

The Nortel WLAN 2300 Series is a complete 802.11 solution for enterprises wishing to deploy widespread wireless coverage for today's business, IP Telephony and converged multimedia applications. The solution combines the latest industry standards with a centralized architecture and advanced features to create a secure, cost-effective and highly scalable WLAN infrastructure. The WLAN 2300 Series includes the tools and features required for successful planning and implementation, whether deploying a first-time WLAN using a quick and simple approach, or graduating to a precisely engineered mobile infrastructure as part of a global enterprise mobility strategy.

The WLAN 2300 Series features a centralized wireless LAN deployment model with "thin" access points controlled and managed by a central WLAN Security Switch. The series is comprised of four primary elements:

- WLAN Access Points
- WLAN Security Switches
- WLAN Management Software system
- WLAN Location Engine

Each plays a key role in the complete mobility solution.

- The **Nortel WLAN 2300 Series Access Points** perform 802.11a/b/g mobile connectivity, encryption/decryption for wireless traffic, priority queuing and radio frequency (RF) monitoring, including rogue access point identification and containment. Access points exchange control and data traffic with their associated WLAN Security Switch.

- The **Nortel WLAN 2300 family of security switches** controls the access points and performs key functions such as security, networking, quality of service (QoS) and roaming for mobile users. The WLAN Security Switch also correlates radio frequency data from multiple access points and coordinates their response to changing RF conditions and RF attacks.
- The **Nortel WLAN Management Software** system is a comprehensive design and management tool that identifies ideal access point locations on detailed floor plans, configures all devices with a single click and provides granular monitoring and reporting for complete visibility and control over the entire system.
- The **WLAN Location Engine** is an optional element that adds integrated location services to any WLAN 2300 installation enabling new applications and services such as location-based security policies, content delivery or asset locating and tracking.

Support for 802.11n

The introduction of WLAN 802.11n into the marketplace represents an exciting time for customers due to its greatly enhanced capabilities over the

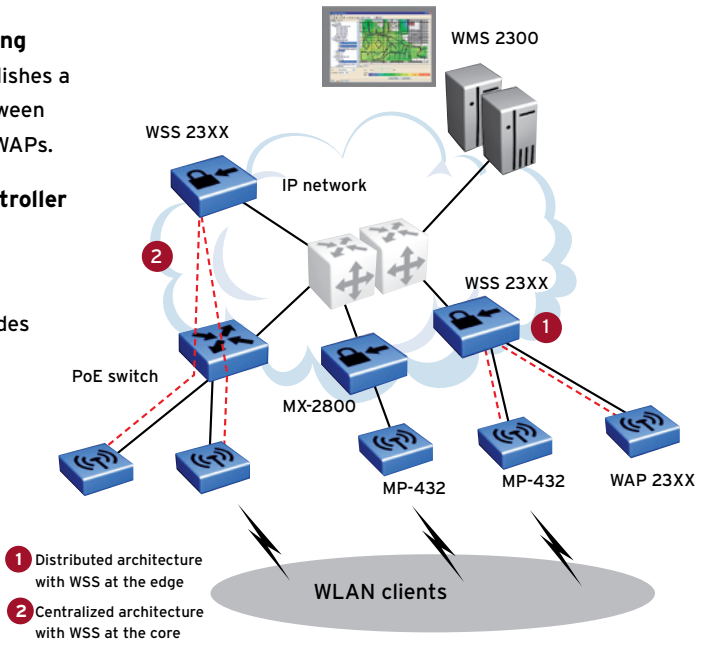
Figure 1. WLAN 2300 Centralized WLAN System

Access Points are dependant on WLAN Security Switch for operation

Control and Provisioning Protocol (CAPP) establishes a secure control plane between a WSS and its managed WAPs.

Trapeze MX-2800 controller for high capacity 802.11n deployments.

Trapeze MP-432 provides the 802.11n wireless interface. It can run on a WLAN 23xx switch and/or the Trapeze MX-2800 controller.



WLAN Management System (WMS) 2300 for system-wide planning, configuration and management

WLAN Security Switch (WSS) 23XX controls the access points and can be deployed either at the edge of the network (1) to support directly connected APs, or elsewhere in the network (2) to support indirectly connected APs across the LAN.

WLAN Access Point (WAP) 23XX provides the 802.11 a/b/g wireless interface and can be directly connected to either a PoE switch, or a WSS. Each WAP is dependant on a WSS for operation.

existing 802.11 a/b/g standards, in terms of capacity, range and reliability. Refer to Figure 2 for an 802.11 a/b/g/n comparison. As part of WLAN 2300 Release 7, Nortel is introducing two Trapeze branded products — an 802.11n Access Point (Trapeze MP-432) and a new high-capacity switch (Trapeze MX-2800). The Trapeze MP-432 AP will run on existing WLAN 23xx security switches. These are optional products, intended for those customers with an immediate need for 802.11n.

Nortel's recommendation is that before installing any new technology, particularly one based on a draft standard, it is important for customers to first consider all of the implications and create an approach that meets the needs and business goals of your organization.

Deploying 802.11n involves much more than just an exchange of hardware and software. A wide range of issues need to be carefully considered (sidebar below), and developing a comprehensive plan spanning applications, clients and infrastructure is recommended. Refer to the Nortel white paper "Ten factors to consider before deploying 802.11n" (available for download at www.nortel.com/wlan) for additional information.

Considerations for 802.11n adoption

- Application drivers
- Risk comfort level
- Support strategy for clients
- Controller processing
- Access point powering
- LAN considerations
- Deployment planning
- Budget
- Timing
- Vendor selection

Figure 2. 802.11a,b/g,n comparison

	802.11b	802.11g	802.11a	802.11n*
Compatibility	802.11b	802.11b,g	802.11a	802.11a,b,g,n
Number of channels	3 non-overlapping	3 non-overlapping	Up to 15 non-overlapping channels (country specific)	Same as 802.11 a/b/g using 20 MHz channels. Restricted to 1 in 2.4 GHz and 3 in 5 GHz using 40 MHz channels
Typical Indoor range	100 ft - 300 ft	100 ft - 300 ft	40 ft - 300 ft	Expected to be 2X range of 802.11a/b/g
Typical outdoor range (Line of sight)	400 ft - 1500 ft	400 ft - 1500 ft	100 ft - 1000 ft	N/A
Data rates	11, 5.5, 2 and 1 Mbps	54, 48, 36, 24, 18, 12, 9 and 6 Mbps	54, 48, 36, 24, 18, 12, 8 and 6 Mbps	Up to 600 Mbps (up to 300 Mbps in WLAN 2300 R7)
Wireless medium	DSSS, 2.4 GHz	OFDM, 2.4 GHz	OFDM, 5 GHz	OFDM-MIMO in 2.4 and/or 5 GHz

* Ratification of standard expected 2H 2009

Nortel's WLAN 2300 Series advantage

A better user experience

The WLAN 2300 Series provides best-in-class performance to support delay-sensitive applications like voice and multimedia. Seamless, fast roaming among all access points, dynamic RF management and QoS policy enforcement means that users get the highest quality WLAN experience possible — a must for IP Telephony and multimedia applications.

A better administrative experience

The WLAN 2300 Series makes life easier for administrators by automating tasks throughout the entire implementation and operations life cycle. The WLAN Management Software system provides an analytical site survey that considers three-dimensional RF attenuation characteristics of all elements that will impact WLAN coverage. Competing approaches often apply open-air scenarios to indoor floor plans without any adjustment for structure and materials.

The broad family of WLAN Security Switches means that the right model can be deployed for any scenario. The access points automatically find and connect to WLAN Security Switches, and flexible AAA, QoS and security enforcement options allow for a seamless fit with existing policy structures and security equipment. The WLAN Management Software system also adopts new access points and WLAN Security Switches into an updated Wireless LAN topology.

Real-time RF management handles unpredictable user loads and interference without the need for administrator intervention, and unlike competing solutions, the WLAN 2300 Series puts client performance first so that channel and power adjustments don't disconnect active users. And extending the architecture to remote branch offices couldn't be easier. WLAN Security Switches self-configure and ensure that WLAN service stays up even if WAN links fails.

The WLAN 2300 Series even makes visitor-based networking a breeze. A unique streamlined application designed for front-desk personnel can be used to generate temporary guest IDs with expiration times and pre-configured access controls.

As for security, the WLAN 2300 Series goes beyond the latest industry security standards with built-in wireless threat protection that guards against RF-based attacks and vulnerabilities. The advanced RF scanning and control capability protects against unauthorized access points and ad-hoc users. Even the WLAN components themselves are authenticated before they're accepted into the system and all subsequent control traffic is encrypted. And to make sure that the WLAN doesn't add another layer of policy administration, the system will pull user policies directly from existing backend AAA servers, and bind those policies to users as they roam. Working together, the vast range of security capabilities ensures that user mobility doesn't compromise the integrity of your network services.

A better return on your mobility investment

The number one expected benefit from WLAN investments is improved user productivity — which can only be realized if the WLAN service and supported applications perform to the user's expectations. And usage patterns are changing quickly. Users are connecting more frequently with WLAN and staying connected longer than ever before. Add to this a parallel investment in IP Telephony and converged applications, combined with convenient desktop videoconferencing and the onslaught of new and embedded 802.11 clients, including dual-mode cellular/Wi-Fi® phones, and it's clear that demand for voice and multimedia over WLAN is imminent.

Dynamic RF management capabilities of the WLAN 2300 Series

Dynamic channel assignment — Access point radio channels are adjusted to optimize user performance when RF conditions change.

Dynamic interference avoidance — Access point radio channels and power levels are adjusted to compensate for unexpected sources of interference.

Dynamic user load balancing — Client-to-access point associations are adjusted to optimize user performance during peak usage periods.

Dynamic power control — Access point radio power transmission levels are adjusted to optimize user performance when RF conditions change.

Dynamic coverage hole protection — Neighboring access points increase power levels and adjust channels to compensate for an unexpected outage.

Whether you're planning to adopt Voice over Wireless LAN today, or tomorrow, the WLAN 2300 Series is designed to deliver high-quality voice and converged services that are necessary to achieve real user productivity improvements. The system offers multiple levels of redundancy not found in competing solutions — access points can be dual-homed to find a backup connection should one fail, and WLAN Security Switches can be deployed in an active-standby configuration with n+1 redundancy and offer dual power supplies as well. Dynamic RF management, rogue access point protection and wireless threat protection will keep today's mobile services and applications up and running during worst-case scenarios. Even the granular monitoring and reporting tools have been specifically designed for administrators who need to support business-critical services.

WLAN Security Switch 2300 Series

The WLAN 2300 Series includes a family of security switches, each designed to meet specific needs of enterprise-wide deployments. The portfolio breadth, combined with advanced features and a common management system, provides unparalleled deployment flexibility and scalability to meet the growing demands of mobile professionals. Each switch can be deployed and managed independently, or can participate with other 2300 Security Switches in large enterprise network deployments. In multiple switch architectures, client information and policies are shared among switches to permit fast roaming among all access points. Regardless of network size or topology, the WLAN Security Switch 2300 family can lower equipment costs substantially by offering the right-sized product for any deployment scenario.

- **Nortel WLAN Security Switch 2350**
  The WLAN Security Switch 2350 is the smallest switch in the 2300 Series and is ideally suited for extending WLAN services to small or branch office environments. The WLAN Security Switch 2350 auto-configures when first connected to the network and can control up to three access points. It offers the same features as the larger 2300 switches but in a smaller package.
- **Nortel WLAN Security Switch 2360**
  The WLAN Security Switch 2360 is ideally suited for mid-size office sites or wiring closet deployments and can control up to 12 access points that can be either connected directly to one of the eight Ethernet ports or indirectly through a Layer 2 or 3 network. The WLAN Security Switch 2361 is identical to the 2360, but adds a second power supply for improved wireless service resiliency.
- **Nortel WLAN Security Switch 2382**
  The largest switch in the 2300 series features Gigabit connectivity and is designed for large deployments and data center installations. The WLAN Security Switch 2382 can be licensed to control up to 128 distributed access points. Dual power supplies provide superior resiliency for voice and business applications.

User-based policies for enhanced security

WLAN Security Switches can enforce security and QoS policies based on the individual user or group identity — not their device, initial access point or physical port. These policy assignments can be maintained locally, or pulled from central AAA servers during authentication. The latter approach allows for massive scale and stronger security by centralizing policy management and mitigating the need to update and synchronize multiple policy databases. Subsequent to authentication, user policies are propagated to other WLAN Security Switches to allow for fast, secure roaming with consistent QoS levels. The WLAN Security Switch tracks and maintains records of user location, roaming history, data transferred and other activity for accounting and billing purposes.

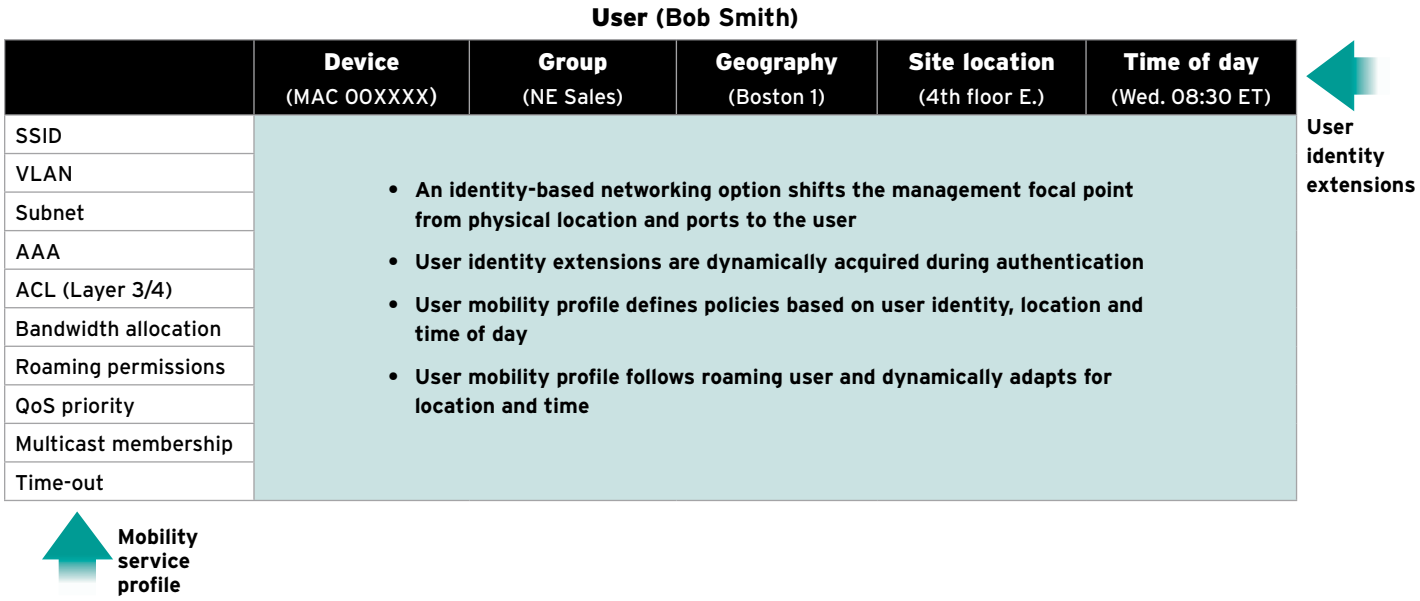
Mobility domains for "free" roaming

Each WLAN Security Switch controls a specified number of access points which in turn creates an 802.11 service domain where mobile users can roam freely. Multiple WLAN Security Switches can work together to create large mobility

Figure 3. WLAN Security Switch options

	WSS 2350	WSS 2360	WSS 2361	WSS 2382	MX-2800
Number of Fast Ethernet ports/ Power over Ethernet	2/1	8/6	8/6	1/0 (Mgt)	1/0 (Mgt)
Number of Gigabit Ethernet ports	–	–	–	2 x 1-Gbps (SFP)	8 x 1-Gbps (RJ-45 or SFP) 2 x 10-Gbps (XFP)
Number of access points supported	3	12	12	Licensed N x 32 128 max	Licensed N x 64 512 max
Third-party AP support	Yes	Yes	Yes	Yes	Yes
Form factor	Small table mount	1U rack mount	1U rack mount	1U rack mount	1U rack mount
Power supply	Single	Single	Dual-redundant	Dual-redundant	Optional Dual-redundant
Application	SMB/ branch office	Mid-size office/ wiring closet	Mid-size office/ wiring closet	Data center	Data center

Figure 4. Mobility management — Control of the mobility domain



domains that can span multiple floors, an entire building or campus. Within the mobility domain, each user's security, QoS and access policies follow them as they roam from access point to access point. Regardless of where a user roams, their traffic will always be tunneled back to the WLAN Security Switch that can put them on to the appropriate network VLAN and subnet. This roaming architecture ensures a symmetrical data flow and won't break multi-cast memberships like competing solutions.

Virtual service groups for management flexibility

Each WLAN Security Switch can support up to 32 independent virtual WLANs over a single infrastructure. Each virtual WLAN can be set up as a unique service group that can be assigned its own VLAN, subnet and AAA server(s), along with specific security and QoS policies. In shared environments or managed services implementations, each virtual service group can have its own Web authentication page to request usernames and passwords or display instructions, welcome banners, corporate identities or advertisements.

AAA management/offloading offers authentication options

WLAN Security Switches are capable of enforcing multiple authentication options including client MAC address, 802.1X or Web-based authentication, and can map any SSID or virtual service group to a primary and backup AAA server, or load balance requests among multiple AAA servers for service resiliency. The WLAN Security Switch offloads back-end AAA servers by terminating and processing Extensible Authentication Protocol (EAP) for 802.1X users, including key generation and management functions for EAP-TLS, EAP-MD5 and PEAP. The WLAN Security Switch will also offload Transport Layer Security (TLS) processing, including X.509 certificate generation and management.

Centralized access point management provides simplified administration

Each WLAN Security Switch provides centralized management for the access points under its control. Firmware updates, configuration changes and RF management can all be performed by the WLAN Security Switch through a management interface or via Wireless Management Software. The WLAN Security Switch management system provides administrators with detailed tracking and reporting of activity on all access points.

Dynamic RF management ensures optimal coverage

The WLAN Security Switch continually receives RF data from associated access points and processes important information such as traffic load, interference from nearby devices, noise levels, client signal strength and signal-to-noise ratios. Using this data, the WLAN Security Switch calculates the optimal 802.11 channel assignments and radio power transmission levels for all associated access points. The WLAN Security Switch can automatically apply these settings to the respective access points and keep the WLAN system operating at peak performance and efficiency even when adverse or unexpected conditionsarise such as outages, interference or radio jamming attacks.

User RF optimization provides personalized performance

The WLAN Security Switch 2300 Series takes RF management to a new level by assimilating client RF data and client

usage patterns, in addition to the basic RF data received from access points. The result is an auto-tuned RF environment that is optimized for user performance and usable capacity rather than blind approaches that achieve a theoretical balance among access points. By focusing on user performance, the WLAN 2300 keeps access points optimized for voice, multimedia and business applications.

Plug-n-Play/Plug-n-Grow

Traditional standalone WLAN deployments require careful planning and time-consuming reconfigurations of nearby access points whenever new ones are added to the network. The WLAN 2300 Series greatly simplifies this process by immediately recognizing new access points and dynamically incorporating them into the WLAN system with greatly minimized administrator intervention.

Rogue access point protection contains threats

WLAN Security Switches continually monitor RF activity and can identify unauthorized access points and clients that are broadcasting in the 802.11 radio spectrums. The system can identify and locate rogues, alert administrators, monitor the access point's activity and even contain the threat by launching containment measures from neighboring access points. The system can also mirror suspicious wireless traffic on a user or group basis for security scanning.

Enhanced wireless threat protection goes beyond standards

Most of the recently introduced WLAN security standards like WPA2 and 802.11i address concerns relating to user authentication and data confidentiality/integrity, but have done little to protect against RF-based attacks that focus on the WLAN infrastructure itself. The WLAN Security Switch 2300 series can protect against such attacks by comparing current RF activity to a built-in signature database and alerting administrators of a threat and location of the threatening device.

Control of third-party access points

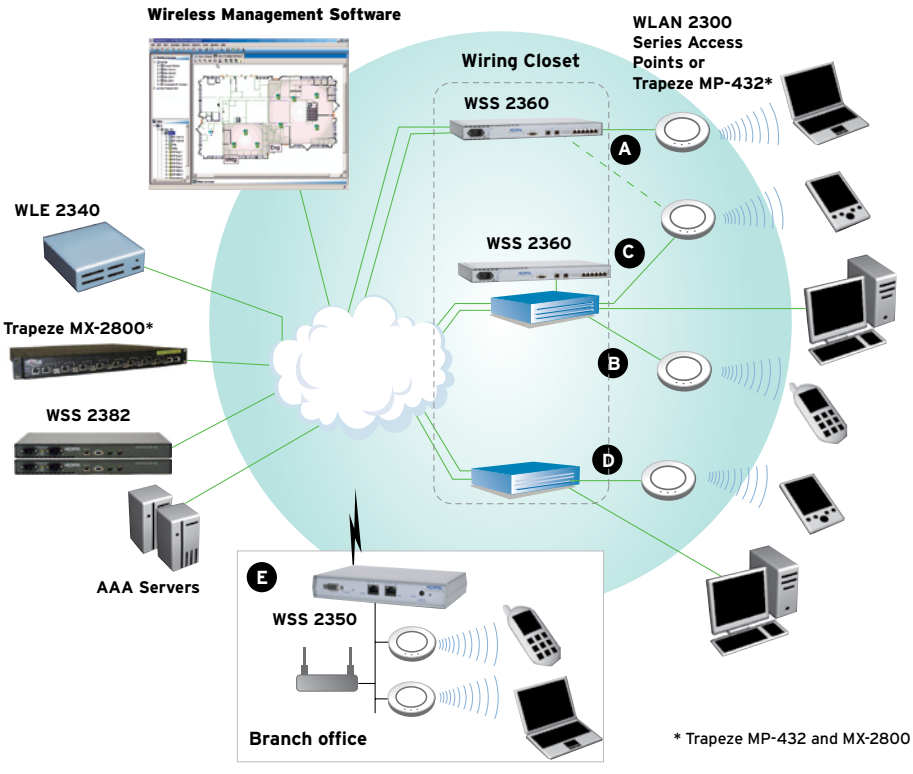
WLAN Security Switches have the unique capability of being able to control popular standalone access points from other vendors. This allows IT departments to keep their existing access points and upgrade to a centralized architecture with many of the benefits of a complete WLAN 2300 system, including user-based policy enforcement and fast roaming.

User load balancing for best performance

Large-scale WLANs can present mobile clients with multiple points of connectivity at any given time. If too many

Figure 5. Multiple deployment options

Seamless integration with existing networks



WAP-WSS configurations

A	Directly connected to WSS 2300
B	Indirectly connected to WSS (in wiring closet) through edge PoE switch
C	Redundant connection using dual-Ethernet ports
D	Indirectly connected to WSS (in data center) through PoE switch
E	Branch office deployment using WSS 2350

* Trapeze MP-432 and MX-2800 hardware requires WLAN 2300 Release 7 software.

Figure 6.
WLAN Access Points

Feature	Nortel WAP 2332	Trapeze MP-432	Others
Dual radio 802.11n (3x3 MIMO)	No	Yes	Yes
Dual radio 802.11a/b/g	Yes	No	Yes
P-MP Wireless Bridging	Yes	Yes	No
Dual Ethernet ports	Yes	Yes	No
Local traffic forwarding	Yes	Yes	No
Fully compatible with existing WLAN 2300 systems	Yes	Yes	No

users connect to a particular access point, individual performance suffers and system capacity is reduced significantly. The WLAN 2300 Series continually monitors user load and will automatically redirect new users to alternative access points and deliver the best possible user performance for given conditions.

Seamless fast roaming enables uninterrupted voice and multimedia services

The WLAN 2300 Series allows seamless roaming between all access points. Mobile clients can roam between access points belonging to different subnets and even between those managed by a different WLAN Security Switch. Additionally, each user's authentication information and associated policies are shared with other 2300 Series Security Switches so that the delay of re-authentication during roaming is eliminated. This allows users to maintain a voice quality connection while roaming within a particular area, between floors and even building-to-building.

Self-healing, resilient design minimizes service disruption

Each WLAN Security Switch maintains a map of RF characteristics within its service domain. In the event of an access point failure, the WLAN Security Switch will immediately recognize the change in RF patterns and respond by increasing transmission power levels of surrounding access points to fill the coverage hole. Similarly, if an access point is temporarily handicapped by a physical obstruction, the system will respond to minimize service disruption. The WLAN Security Switch hardware is also designed for resiliency with dual power supplies, Multi-Link Trunking, active-standby architecture options and n+1 redundancy for access point connectivity to eliminate any single points of failure within the system.

Clustering Support

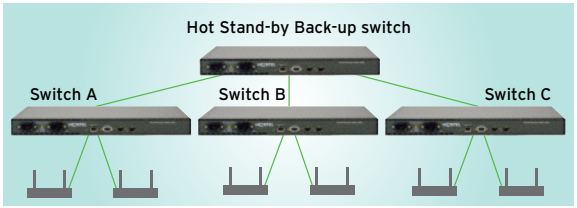
Security switches can be configured in a cluster allowing them to act as a single virtual switch for wireless configurations and AP load balancing, which provides for automatic redundancy. This makes it easier to scale and improves resiliency. This capability solves most of the problems often faced by large-scale enterprises by providing a single point of configuration, automatic AP failover without client connection loss and AP load balancing.

WLAN 2300 Series Access Points

The WLAN Access Point 2332 is a multi-mode, dual-radio 802.11 a/b/g unit. It is controlled by the WLAN Security Switches and can be deployed in large

Figure 7. Clustering diagram

Today's limited approach

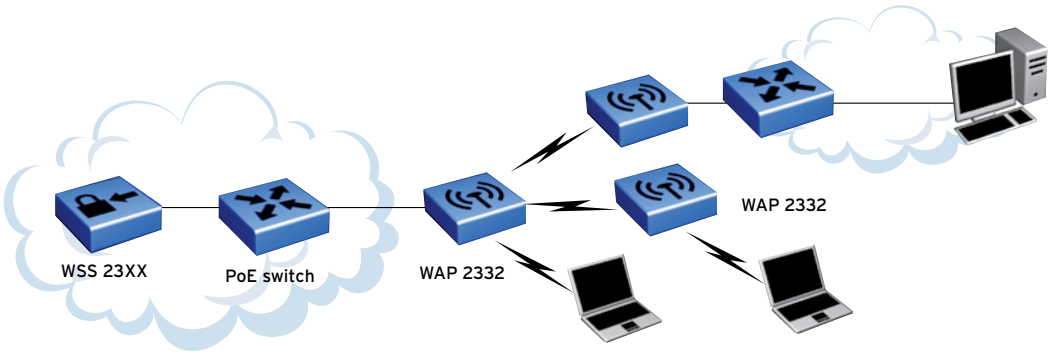


Clustered approach

Discrete switches operate independently	>>>>>	Clustered switches — act collectively as single virtual switch
Harder to scale	>>>>>	Easy to scale — Capacity can be added in chunks, anywhere in the network
Limited resiliency — APs mapped directly to switch	>>>>>	Highest resiliency — APs dynamically map to switches — optimized, auto AP load balancing
Difficult to manage, highest cost of ownership	>>>>>	Easiest to manage, lowest cost of ownership

Figure 8. Wireless backhaul

The WLAN Access Point 2332 can create wireless backhaul links with its neighbors for simpler installations and bridging applications.



numbers without creating a management burden. The APs are plenum-rated for ceiling installations and feature an attractive enclosure that resembles a common smoke detector to blend in with office environments. The Trapeze MP-432 is a dual-radio 802.11n unit. It is fully compliant with the 802.11n Draft 2 standard.

Simple installation

The WLAN Management Software system can be used to map the location of access points based on the expected number of users and type of applications being accessed. The WLAN Management Software system will also calculate each access point's ideal configuration and push it out to the WLAN Security Switches which automatically configure the access points upon installation. The access points can connect directly to an Ethernet port on the WLAN Security Switch, or indirectly across a Layer 2 or 3 network and receive 803.3af Power over Ethernet (PoE) from a WLAN Security Switch, a PoE capable Layer 2/3 switch or PoE injector.

Resiliency and QoS for voice and multimedia applications

The WLAN 2300 series Access Points are designed to deliver reliable service for voice and multimedia applications and feature redundant Ethernet ports that allow for a backup network connection if the primary port fails for any reason.

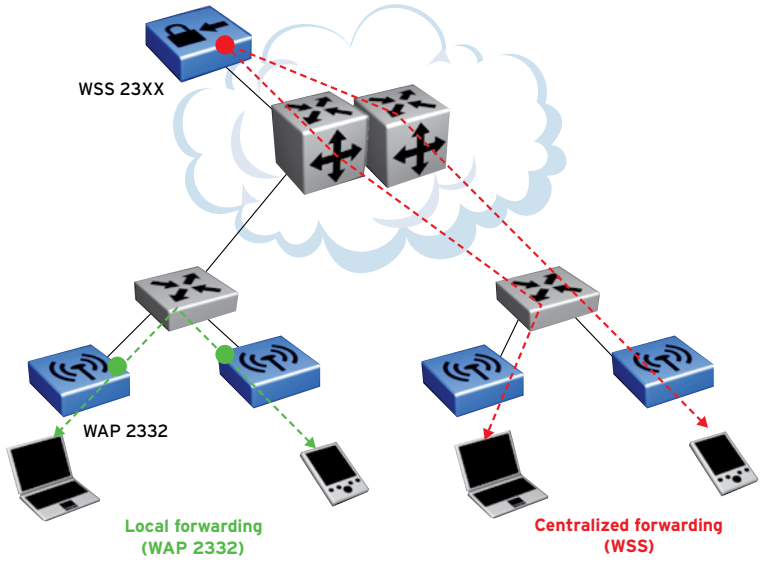
To deliver the best user experience, the access point classifies traffic into multiple user and group queues based on AAA-defined QoS policies, SVP or DiffServ classifications. The access point does not store any sensitive security information locally, making it safe for unsecured areas, and if theft is still a concern, then each access point can be physically locked down using the Kensington™ lock interface. To prevent tampering, each access point is authenticated to a WLAN Security Switch upon installation and all subsequent control traffic is encrypted.

RF scanning to prevent unauthorized activity

The WLAN 2300 series Access Points can perform scheduled or automated RF scans to search for unauthorized 802.11 devices and detect RF attacks. Access Points can run periodic sweeps of all channels in the active radio band while simultaneously providing mobile connectivity, or they can act as dedicated RF monitors and scan all

Figure 9. Local traffic forwarding

The WAP 2332 has the unique ability to import a user's policies from the WSS and forward traffic locally, outside of the WSS tunnel. This option can improve system capacity by offloading the WSS of excessive data traffic and can improve performance by creating shorter data paths.



bands and channels continuously. Any unauthorized activity or unexpected change in RF conditions is reported to the WLAN Security Switch, which determines if a rogue access point has been identified or if channel or power level adjustments are required.

Flexible antenna options for customizing signal patterns

The WLAN 2300 series Access Points are equipped with dual internal radios, omni-directional dual diversity antennas with external antenna connectors that allow enterprises to customize signal patterns and match particular deployment requirements.

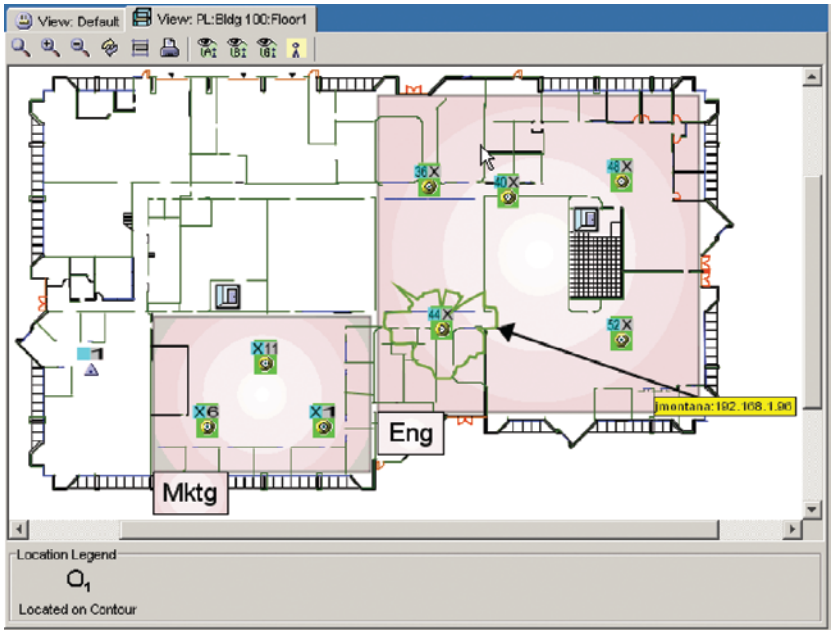
WLAN Management Software system

The WLAN Management Software system is much more than a management application — it is an integrated tool suite that helps administrators through every phase of the project cycle from initial planning, deployment and configuration through ongoing operations support, troubleshooting and reporting. WLAN Management Software runs on common server platforms including Windows 2000, Windows XP and LINUX, and can support hundreds of individual WLAN Security Switches and thousands of access points. The WLAN Management Software system lets administrators perform system-wide updates with a single key stroke and "see" what's happening at any moment with the rich graphical interfaces. The WLAN Management Software system is a client/server application and can support up to four simultaneous administrators, each with individual access levels and authorizations.

Painless planning and deployment

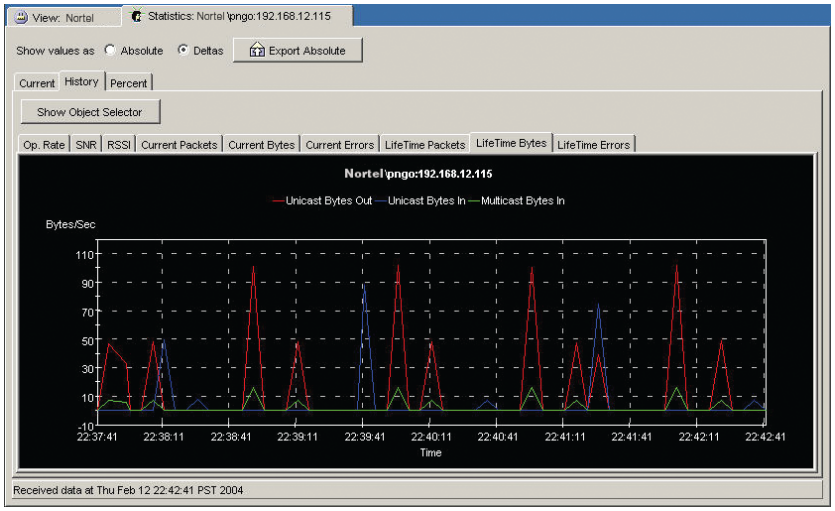
Prior to deployment, the WLAN Management Software system can act as a powerful standalone analytical site survey and planning tool that can import AutoCAD DXF™, AutoCAD DWG, JPEG or GIF floor plan files and apply attenuation characteristics to walls, doors, ceilings and other RF obstacles. The system can then design the ideal WLAN network including topology, equipment counts and radio channel and power settings. It even considers minimum user throughput levels, user volumes, failover and peak capacity scenarios to help engineers build service-ready WLANs for voice

Figure 10. Client and Rogue Access Point Location



The WLAN Management Software system accurately locates clients and rogue access points on imported floor plans.

Figure 11. Detailed Monitoring



The WLAN Management Software system provides an intuitive dashboard for monitoring and troubleshooting. The system provides WLAN topology, element status, RF and client performance information, historical data and more.

Security capabilities of the WLAN 2300 System

Security standards/authentication

- WPA/WPA2
- 802.11i/802.1x
- EAP-TLS, EAP-TTLS, EAP-MD5, EAP w/MS CHAP v2 and PEAP, PEAP-TLV
- MAC authentication
- X.509 certificates
- RADIUS AAA
- RADIUS Extensions
- Local AAA
- Web-based AAA

Cryptography

- WEP, dynamic WEP, TKIP: RC4 40/108 bit
- SSL, TLS: RC4 128 bit
- CCMP: AES 128 bit
- Public key cryptography RSA 1024/2048 bit

Wireless threat protection

- Flood attack detection
- RF jamming protection
- AP MAC address masquerading detection
- Weak WEP IV detection
- Spoof attack detection
- Rogue AP protection

Access control

- User/group identity
- Multiple SSID
- MAC filtering
- Layer 3 deny filters
- Layer 4 deny filters
- Time-of-day restrictions
- Day-of-week restrictions
- Location-based policies
- Client blacklisting
- Subnet classification
- VLAN assignments
- Roaming restrictions

Rogue access point protection with the WLAN 2300 Series

- Rogue access point detection — Unauthorized access point is detected during an RF scan.
- Rogue access point alert — Notifies the appropriate administrator of the event.
- Rogue access point classification— Analyzes and classifies the threat based on behavior.
- Rogue access point location — Identifies access point location on the floor map.
- Rogue access point monitoring — Records behavior and usage.
- Rogue access point containment — Threatening access point is crippled by an RF attack.

and converged applications. The WLAN Management Software system will map the access point's physical location on floor plans and produce an accurate bill of materials to make installation as simple as possible, and once access points are installed, it can push configurations out to thousands of devices with a single key stroke to get the WLAN up and running as quickly as possible.

The system can also import RF maps from an Ekahau™ site survey tool and overlay them on top of existing floor plans for an exact RF topology and more accurate rogue access point and user location. An open API can be used to export user location to third-party applications.

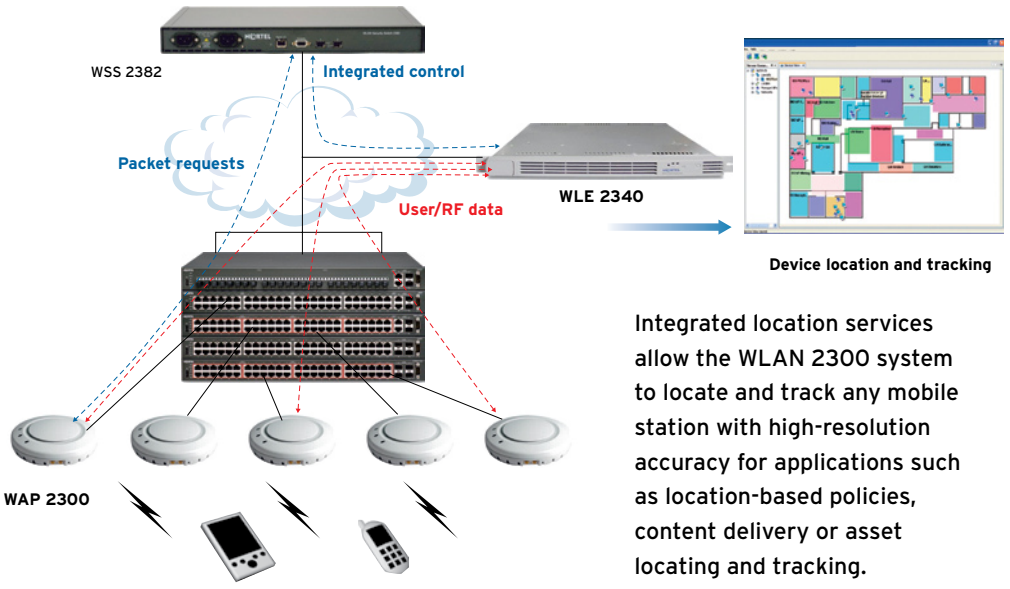
Ongoing operations

The WLAN Management Software system is designed to equip administrators with the powerful tools required to support wireless voice and converged services. The visual interface presents a top-level floor plan view that includes RF topology, access point, rogue access point and user location mapping with configurable alarms for ongoing monitoring of the WLAN. Should an event occur, administrators can troubleshoot by drilling down to a granular level and see user roaming and usage history, RF and network statistics and hierarchical maps. The threat of rogue access points and ad-hoc users is mitigated through immediate identification, location and containment. All user, network and RF data, statistics and history can be captured in customizable reports and the planning tool can also be used on an ongoing basis to support configuration updates and new equipment deployments as the network grows. The WLAN Management Software system also features an HP OpenView plug-in to integrate with existing management systems.

WLAN Location Engine

The WLAN Location Engine 2340 is an integrated location services solution that uses the RF and user data captured by the WLAN 2300 access points to resolve the location of thousands of mobile stations or asset tags simultaneously.

Figure 12. WLAN Location Engine 2340



Integrated location services allow the WLAN 2300 system to locate and track any mobile station with high-resolution accuracy for applications such as location-based policies, content delivery or asset locating and tracking.

This capability can be used to strengthen security with zone-based access controls, enable new services such as location-specific content delivery, or as the foundation for new applications like asset tagging, locating and tracking. An application programming interface makes the location information accessible for any business application that can benefit from user location.

WLAN 2300 Accessories

The WLAN 2300 series supports a range of antennas for both indoor and outdoor use. This allows for improved deployment flexibility where planners can choose an antenna pattern that meets coverage requirements while allowing for convenient AP placement and installation. Customers may use outdoor antennas for fringe coverage around and between buildings on an enterprise campus. This allows customers to extend their wireless LAN services outdoors, allowing them to enjoy the benefits of a single management system for outdoor use in courtyards, parking lots, the exteriors of a warehouse for shipping and control applications. Other applications include outdoor Internet access, security cameras, facilities dispatch and environmental controls. Optional power supplies are also available.

Optional 802.11n hardware

Trapeze Networks MP-432 (802.11n Access Point)

The Trapeze Networks indoor MP-432 is a high-performance 802.11n (3x3) Multiple Input/Multiple Output (MIMO), dual radio access point, with maximum aggregate data rates of up to 600 Mbps. One radio operates in the 2.4 GHz band and one in the 5 GHz band. The MP-432 is backwards compatible with legacy 802.11 a/b/g clients in the 2.4 GHz and 5 GHz bands to provide investment protection without the need for a second overlay networks. It is compliant with the IEE 802.11n Draft 2.0 standard. In most deployment scenarios, the MP-432 operates in full functionality 3 x 3 MIMO dual radio mode with the existing IEEE 802.3af. The MP-432 is compatible with the Nortel WLAN 23xx Security Switches.

Key features include:

- Highest possible performance
- Simultaneous dual band operation (2.4 GHz and 5 GHz)
- 300 Mbps per band up to 600 Mbps total
- 3x3 MIMO in both bands
- Adaptive frame aggregation
- 2 Gigabit Ethernet uplink ports
- Protects existing Wi-Fi investment
- Runs on existing WLAN 23xx security switches
- Works with existing or emerging power standards (802.3af, 802.3at)
- Fits existing mounting brackets
- Wi-Fi certified ready
- Fully compliant with 802.11n Draft 2.0
- Wi-Fi certifiable
- Ensured interoperability with standards-based network

Trapeze Networks MX-2800 (High Capacity Controller)

The Trapeze Mobility Exchange MX-2800 is the next-generation WLAN controller for medium to large-size enterprise WLAN deployments. It offers 28 Gbps of throughput and supports up to 512 802.11n APs, while providing always-on availability and hitless failover with no service interruption.

Key features include:

- 28Gbps Ethernet switching capacity
- 2 10-Gbps ports; 8 1-Gbps ports
- Line-rate speed and throughput
- Industry's only hardware-switched wired and wireless
- 512 active AP's (Note: max 256 AP with software version 7.0; max 512 AP with software version 7.2 or later)
- 12,000 active clients per switch

Why you should choose Nortel's WLAN 2300 Series

Built to support voice and multimedia applications in today's networks

The WLAN 2300 Series is designed for voice, multimedia and business-critical applications; it adheres to the latest QoS standards and minimizes the performance impact of today's strong security standards by offloading back-end AAA servers of many cryptographic processing functions. This architecture allows fast secure roaming among all access points with the minimal latency and jitter needed to support time-sensitive applications. Dynamic RF management ensures service resiliency by protecting against unexpected interference, obstructions, outages and weak coverage zones that can have a significant impact on performance and user experience. The system can also be deployed with full redundancy of all network components to protect against service interruption.

Trapeze Networks MP-432

Trapeze Networks MX-2800

Mobility management keeps control over roaming users

The WLAN 2300 Series takes mobility to a higher level by allowing security and QoS policies to follow users as they roam anywhere on the WLAN network. Access controls, VLAN/subnet assignments, bandwidth rate, QoS priorities and multicast memberships are enforced even if the user roams between floors and buildings. Administrators can assign time-of-day restrictions and even location-based restrictions that block access from
specific areas like parking lots or exam and emergency rooms.

Easy implementation — from planning to production

The WLAN Management Software system helps network administrators through every phase of a WLAN project from planning and configuration through to monitoring, reporting, expansion and ongoing operations. Beginning with a basic floor plan, WLAN Management Software builds a visual map of the ideal WLAN network, including radio coverage, physical topology and access point locations. The tool then produces a bill of materials for your implementation and once the equipment is installed, configurations can be pushed out to all system elements with a single key stroke. Granular monitoring and customizable reporting keeps administrators on top of all activity and provides everything they need to handle troubleshooting and support calls for enterprise-wide converged mobile services.

Extend your LAN to wireless with seamless deployment in any network

The WLAN 2300 Series is designed to operate as an overlay to existing IP networks without the need for network reconfigurations or expensive upgrades to core switch infrastructure. The solution can be configured to enforce existing authentication policies and extensions; it does not introduce any new protocols that will impact other devices. The access points can be installed on any subnet or in any wiring closet, allowing the placement to be simple, convenient and focused on providing optimal wireless coverage. Once in place, the access points attach to their controllers across the network, and provide seamless roaming for mobile users, regardless of what subnets the access points are attached to. The mobile user's IP address doesn't change, and applications keep working. For installations that support multiple user types such as hospitals, multi-tenant buildings, airports and college campuses, one WLAN infrastructure can be securely partitioned to form up to 32 unique service groups, each with their own Web-portal, security and QoS policies.

Standards-based/open client approach for user and application compatibility

The WLAN 2300 Series adheres to the latest IEEE and de-facto industry standards to ensure strong security and QoS while maintaining compatibility with user devices. The system supports security standards such as WPA, WPA2, 802.11i/802.1x with WEP, Dynamic WEP, TKIP, CCMP, EAP-TLS, TTLS and PEAP, PEAP-TLV and QoS standards including 802.1p and DiffServ, WMM and SVP. Advanced features such as dynamic RF management, fast roaming and user policy management do not carry any client prerequisites other than the 802.11a or b/g standards present on all adapters and Centrino™ enabled devices. The WLAN Management Software system makes work easy during the planning phase by recognizing floor maps in all common formats, including AutoCAD® DXF™, AutoCAD DWG, JPEG or GIF file types.

Nortel's WLAN 2300 Series is the ideal choice for customers seeking the performance, management tools and resiliency required for delivering high-quality voice and multimedia applications over a wireless network.

Visit Nortel on the Web at **www.nortel.com**. For the latest Nortel news, visit **www.nortel.com/news**.

For more information, contact your Nortel representative, or call 1-800-4 NORTEL or 1-800-466-7835 from anywhere in North America.

NN111046-110608

NORTEL

BUSINESS MADE SIMPLE

In the United States:
Nortel
35 Davis Drive
Research Triangle Park, NC 27709 USA

In Canada:
Nortel
195 The West Mall
Toronto, Ontario M9C 5K1 Canada

In Caribbean and Latin America:
Nortel
1500 Concorde Terrace
Sunrise, FL 33323 USA

In Europe:
Nortel
Maidenhead Office Park, Westacott Way
Maidenhead, Berkshire SL6 3QH, UK
Email: euroinfo@nortel.com

In Asia:
Nortel
United Square, 101 Thomson Road
Singapore 307591
Phone: (65) 6287 2877